Program Charter
For
Information Technology Services

Program Manager: Dennis Morgan
Program Support Sub-Goal Team Lead: William Broglie

1. EXECUTIVE SUMMARY

The Information Technology (IT) Services Program: (1) is the NOAA Chief Information Officer's (CIO's) program; (2) enforces the federal rules and regulations covering the acquisition, management, and use of IT resources; (3) leads the improvement of NOAA operations and service delivery using IT systems; (4) promotes the effective use of IT to accomplish the NOAA mission; (5) provides advice to NOAA management on information resources and information systems management; (6) promotes and shapes an effective strategic and operational IT planning process for NOAA; (7) coordinates preparation of the NOAA IT budget and associated materials; (8) oversees selected NOAA-wide operational IT systems and services; and (9) apportions funding for the NOAA CIO and Line Office CIO operating budgets to improve IT systems across NOAA by providing centralized administration and management of resources.

The NOAA Strategic Plan presents challenges in IT administration, security, network operations, enterprise architecture, and support. Significant investments in hardware, software, and human capital will be required. The strategic objective of the IT Services Program is to develop and maintain a secure, reliable, technically robust operating environment to support the NOAA mission goals and ensure accessibility and the highest data quality for the public. The IT Services Program provides the support that makes the NOAA mission happen.

2. PROGRAM REQUIREMENTS.

A. Requirements Drivers:

The IT Services Program is responsible for implementing the following laws, regulations, and policy:

Clinger-Cohen Act (aka, Information Technology Management Reform Act of 1996)

- This Act was designed to improve the way the federal government acquires and manages IT. It requires the Department and individual programs to use performance-based management principles for acquiring IT. These principles include: (1) planning major IT investments; (2) revising processes before investment; (3) enforcing accountability for performance; (4) using standards; (5) increasing acquisition and incorporation of commercial technology; and (6) using modular contracting.
- This Act established departmental Chief Information Officer (CIO) offices, and placed responsibility for developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture onto the agency CIO.

Federal Information Security Management Act (FISMA, enacted December 2002)

- This Act (Title II of the E-Government Act of 2002) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Agencies are required to report annually on IT Security program implementation of FISMA requirements. This framework drives the policy and investment requirements of the IT Services Program for security and operation of IT systems.

Federal Financial Management Improvement Act of 1996 (FFMIA)

- All administrative financial systems must conform to this Act (Public Law 104-208, Title VIII), which provides for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government in order to increase the accountability and credibility of federal financial management. This requires the IT Services Program to maintain and operate all systems to this standard.

Computer Security Act of 1987

- In this Act (Public Law 100-235), the Congress declares that improving the security and privacy of sensitive information in Federal computer systems was in the public interest, and created a means for establishing minimum acceptable security practices for such systems.

Paperwork Reduction Act (PRA)

- This act requires the IT program to develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions. (Section 3506(b))
- Obtain prior OMB clearance before asking 10 or more members of the public identical questions or issuing information requirements in a rule of general applicability. An office independent of the program office must review all collections prior to submission to OMB. (Sections 3507 and 3506 (c))

Federal Managers' Financial Integrity Act of 1982 (FMFIA)

- This Act (Public Law 97-255) provides requirements for executive agency accounting and other financial management reports and plans, including identification and reporting of material weaknesses (section 2, (d)(4)). In accordance with this Act, the IT Services Program participates in regular audits, risk analysis of major systems, and reporting requirements.

Privacy Act of 1974

- This Act (Public Law 93-579, as amended, Title 5 U.S. Code section 552a) prohibits disclosure of information in personal records by any means of communication to any person or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. This Act requires the IT systems be maintained to prevent disclosure of personal records and information.

Government Paperwork Elimination Act

- This Act requires the IT Services Program to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. Although there is an expiration date, OMB has indicated reporting will continue. (Section 1704)
- Also, to take all steps necessary to ensure that multiple methods of electronic signatures are

available for the submittal of forms if 50,000 or more submittals of a particular form are expected. (Section 1703(b))

Electronic Government Act

- This Act requires the IT Services Program to:
  - Develop performance measures that demonstrate how electronic government enables progress toward agency objectives, strategic goals, and statutory mandates. (Section 202(b))
  - Submit annual report to OMB on E-Government, addressing status of implementation of electronic government initiatives, compliance with the act, and how electronic government initiatives improve performance in delivering programs to constituencies. (Section 202(g))
  - Establish and operate information technology training programs. General requirements are detailed. Standardized information on the IT and information resources management workforce must be collected. (Section 209(b)(2))
  - Develop, document, and implement an agency-wide information security plan approved by OMB. (Section 301 - revision to 3544)
  - Develop and maintain an inventory of major information systems operated by or under the control of the agency. It must identify the interfaces between each such system and all other systems or networks, including those not operated or under the control of the agency. (Section 305(c))

Federal Information Quality Act (Section 515)

- This Act requires the:
  - Issuance of guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by the agency.
  - Establishment of administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency that does not comply with the guidelines issued under subsection.

Rehabilitation Act (Section 508 - Accessibility)

- To comply with this Act, the IT Services Program requires (when developing, procuring, maintaining, or using electronic and information technology) to ensure, unless an undue burden would be imposed, that the electronic and information technology allows individuals with disabilities who are Federal employees to have access to and use of information and data that is comparable to the access to and use of the information and data by Federal employees who are not individuals with disabilities; and individuals with disabilities who are members of the public seeking information or services from a Federal department or agency to have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities.

OMB Circular A-127, Financial Management Systems

- This Circular prescribes policies and standards for the IT Services Program to follow in developing, operating, evaluating, and reporting on financial management systems in accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and the Chief Financial Officers (CFOs) Act of 1990.

OMB Circular A-123, Management Accountability and Control

- This Circular provides required guidance to the IT Services program on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls in accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA).

OMB Circular A-130

- This Circular directs the establishment of the CIO position and identifies specific authorities to be executed
    - Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans (Section 9(a));
    - Advise the agency head on information resource implications of strategic planning decisions (Section 9(a));
    - Advise the agency head on the design, development, and implementation of information resources (Section 9(a));
    - Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources (Section 9(a));
    - Maintain an inventory of the agency's major information systems, holdings, and dissemination products (Section 9(a)(7));
    - Promote effective and efficient capital planning within the organization (Section 8(b)(1));
    - Document its enterprise architecture and submit to OMB (Section 8(b)(2);
    - Establishes a minimum set of controls to be included in Federal automated information security programs.
- This Circular assigns Federal agency responsibilities for the security of automated information and incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives. (Appendix III)

OMB Circular A-11

- This Circular requires the IT Services Program to prepare an annual budget submission for NOAA. This is submitted as OMB Exhibits 53 and 300 on IT systems, the first reporting on the anticipated costs of IT in the agency and the latter being a business case for each system. (Parts 2 and 7)

Department of Commerce (DOC) Policy: Responsibilities of Commerce Operating Unit Chief Information Officers (August 2006)

- The Department of Commerce requires the NOAA CIO to:
    - Ensure that NOAA uses IT to develop the best, most useful, and most effective products and services to support its mission. As part of this process, ensure that Commerce officials have thorough and accurate information to inform IT decision making.
    - Ensure that NOAA's IT Development, Modernization, and Enhancement (DME) projects and Steady State investment initiatives are managed in an efficient and cost-effective manner.
    - Develop, maintain, and facilitate the implementation of a sound and integrated enterprise architecture to achieve interoperability and portability of systems, integration of work processes and information flows, and information exchange and resource

sharing to support strategic goals within NOAA, Commerce and with external partners.
- Ensure the integrity, availability, and confidentiality of NOAA's IT systems.
- Ensure that NOAA's IT systems, including websites, protect the privacy of the public, businesses, and employees and contractors.
- Further the Department's move to an e-government environment, enabling business functions to be conducted electronically and achieving paperwork elimination goals, both in transactions with Commerce's customers and for internal operations.
- Ensure that NOAA maintains a robust workforce of well-qualified IT professionals.
- Ensure and maximize the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by NOAA.
- Ensure that records are created, maintained, safeguarded, and disposed of in accordance with government-wide and Commerce policies and procedures.
- Ensure the accessibility of Commerce's electronic and information technology to people with disabilities, including those with vision, hearing, dexterity, and mobility impairments.

DOC Policy: IT Security Program Policy and Minimum Implementation Standards (June 2005)

- This document specifies and explains the DOC Information Technology (IT) security program requirements and provides minimum mandatory standards for the implementation of IT Security Programs within DOC. It incorporates by reference the requirements of Federal and Departmental IT Security Laws and Federal Regulations.
- The DOC IT Management Handbook, authorized by Department Administrative Order (DAO) 200-0, incorporates this IT Security Program Policy and thereby provides the IT Security Program Policy the same force and effect of a DAO. This policy establishes the foundation of comprehensive rules and practices that regulate access to an organization's IT systems and the information processed, stored, and transmitted by them. Good policy protects not only information and systems, but also individual employees and the organization as a whole. As such, this policy represents the Department's strong commitment to IT security.

B. Mission Requirements:

The IT Services Program mission requirements are to:

- Acquire and implement information technology infrastructure that assures NOAA missions are able to adequately and securely deliver their data products;
- Provide a technology working requirement that enable NOAA to deliver effective products and services; and
- Assure a fully managed portfolio of all NOAA Information Technology investments in accordance with all mandated rules and regulations.

3. LINKS TO THE NOAA STRATEGIC PLAN

A. NOAA Strategic Goal:

- Provide Critical Support for NOAA's Mission

B. Goal Outcomes:

- A safe operating environment with efficient and effective financial, administrative, and

support services
- Secure, reliable, and robust information flows within NOAA and to the public

C. Goal Performance Objectives:
- Improve efficiency and performance in the processing of financial and administrative transactions and services
- Increase internal and external availability, reliability, security, and use of NOAA information technology and services

D. Goal Strategies:
- Develop and maintain an Information Technology Enterprise that does the following:
  - Fully supports the life cycle of NOAA programs;
  - Is secure, reliable, and cost-effective;
  - Encourages information sharing; and
  - Complies with all applicable polices.

4. PROGRAM OUTCOMES

An IT Enterprise that: (1) fully supports the life cycle of NOAA programs; (2) is secure, reliable, and cost-effective; (3) encourages information sharing; and (4) complies with all applicable policies.

5. PROGRAM ROLES AND RESPONSIBILITIES.

This program is established and managed with the procedures established in the NOAA Business Operations Manual (BOM). Responsibilities of the Program Manager are described in the BOM. Responsibilities of other major participants are summarized below:

A. Participating Line Offices Responsibilities:

1. Individual Line/Staff Offices are responsible for developing individual Line/Staff Office plans and participating in the development of the NOAA Enterprise Architecture. NOAA personnel participate in the enterprise network advisory committee, and manage perimeter networks that are connected to the IT Services Program network operations center.

2. Individual NOAA Programs execute certification and accreditation of systems within their Line/Staff offices and submit all reports to the NOAA CIO. This includes IT security and submission of applicable IT planning information to the NOAA CIO for the establishment of the enterprise level security for intrusion detection and firewalls. Line/Staff Office IT Security Officers assure compliance within their programs and report to the NOAA IT Security Officer who in turn is accountable to the DOC IT Security Officer.

3. The NOAA CIO Council provides policy and direction for NOAA enterprise investments and is responsible for setting priorities.

4. The NOAA Office of General Counsel (GC) is responsible for providing legal services necessary to enable the program to discharge its duties. In this regard, NOAA GC provides a variety of specific services on an as-needed basis, including, but not limited to: advice on legal

issues related to program responsibilities; review and clearance of agreements, testimony, correspondence, and other documents; legal representation; assistance with litigation and requests for testimony or information; and coordination on behalf of the program with the DOC GC in the areas of contract, grant, intellectual property, labor and employment, appropriations, legislation and regulation, grant, litigation, and telecommunications law.

B. External Agency/Organization Responsibilities:

OMB and DOC provide explicit guidance on what is expected to be provided in terms of management reporting, best practices and approved projects. This includes, but is not limited to, dollar thresholds, project management skill requirements, standards, periods of reporting, and performance measurement.

6. END USERS OR BENEFICIARIES OF PROGRAM

A. NOAA managers/personnel: Secure and reliable information provide NOAA personnel and managers confidence in their ability to execute their mission with control and understanding of risks from compromise or support infrastructure failure;

B. Management Information Systems support NOAA processes by infrastructure design;

C. NOAA benefits from risk-based assurance that the agency is meeting regulatory requirements and that investments are funded in a priority commensurate with mission needs and in accordance with the **Capital Planning and Investment Control process.**

D. Academia: System availability and reliable information delivery assists researchers in their endeavors.

E. General Public: Greater and more consistent availability of data and information enables NOAA to meet public demand.